Security of coherent state quantum cryptography in the presence of Gaussian noise

Matthias Heid and Norbert Lütkenhaus
Quantum Information Theory Group, Institut für Theoretische Physik I and Max-Planck Research Group, Institute of Optics, Information and Photonics, Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany
Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, 200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada
(Dated: February 1, 2008)

We investigate the security against collective attacks of a continuous variable quantum key distribution scheme in the asymptotic key limit for a realistic setting. The quantum channel connecting the two honest parties is assumed to be lossy and imposes Gaussian noise on the observed quadrature distributions. Secret key rates are given for direct and reverse reconciliation schemes including postselection in the collective attack scenario. The effect of a non-ideal error correction and two-way communication in the classical post-processing step is also taken into account.

PACS numbers:

I. INTRODUCTION

The goal of quantum key distribution (QKD) is to distribute a key between two honest parties, usually called Alice and Bob, which is provably secure against any eavesdropper Eve. It is assumed that Eve is only limited by the laws of physics. From a practical point of view, implementations using coherent states as input signals and variations of homodyne [1, 2, 3, 4, 5, 6] detection seem to be promising, since they can readily be realized experimentally. Moreover, it has been suggested that homodyne detection can be performed at high repetition rates in continuous variable (CV) QKD to boost the secret key rate [1]. The security of these schemes has been investigated before [1, 7, 8, 9, 10, 11, 12, 13, 14, 15] and unconditional security has been proven for losses of up to 1.4 dB [16]. Though advancing our understanding of these schemes, no analysis has been provided that would give an unconditional secure key over channels with higher losses or channels imposing excess noise on the observed quadratures. In this article we will present an analysis that derives a security result under the assumption of collective attacks and the observation of Gaussian noise. The result is derived in the infinite key limit, thus ignoring statistical effects. Though restricted in this sense, there are strong indications that these restriction can be lifted, so that our results, if successfully combined with other results will lead to the desired unconditional security. We expect this will be a fair representation of the (still missing) full unconditional security proof. We compare different techniques of extracting a secret key from shared classical data such as postselection (PS) and reverse reconciliation (RR). Moreover, our approach can be modified to include two-way communication in the classical post-processing step of the protocol and non-ideal error correction.

Any QKD protocol can be thought of consisting of two phases. The goal of the first phase is to distribute an effectively entangled state between Alice and Bob [17, 18]. This entanglement does not need to be present in actual physical systems. Instead, it can be brought in as a theoretical construct [17, 19], as explained in more detail in Sec. III. In practise, Alice and Bob will use a prepare-and-measure scheme, where Alice encodes some bit-value i into non-orthogonal signal states. She sends a sequence of n such states over the quantum channel to Bob. In general, Eve might interact coherently with these n states. We restrict ourselves here to the case of collective attacks, where Eve attaches an independent probe to each signal. Then the total state shared between Alice and Bob will be of tensor product form $\rho_{AB}^{\otimes n}$.

Eve, however, may keep her quantum states $\rho_{E,i}$, which summarize all her knowledge about the sent signals until the second phase of the protocol is completed. In this phase, Alice and Bob use an authenticated but otherwise insecure classical channel to correct for errors in their bit-strings and to cut out Eve's knowledge about the key (privacy amplification)[20]. The information sent over the classical channel becomes available to Eve who then can optimize her collective measurements on the quantum states. For this scenario of collective attacks, we apply the generic approach by Devetak and Winter [21] to give a lower bound on the secret key rate.

The security analysis presented here applies to the situation where the quantum channel connecting Alice and Bob is lossy with single-photon transmittivity η and imposes Gaussian excess noise δ on the quadrature distributions. This kind of noise is typically seen in the experiments [22, 23]. It has been shown that a distillation of a secret key in CV-QKD is only possible when

$$\delta < 2\eta \,, \tag{1}$$

because otherwise the correlations between Alice and Bob could have originated from a separable state [7]. Here, the excess noise δ is determined via homodyne measurements. It can easily be verified that our calculated lower bounds on the secret key rate for the various types of protocols are well in the regime of quantum correlations.

In this article, we compare different approaches to distill a key for a CV prepare-and-measure scheme. We assume that the quantum channel between Alice and Bob can be verified to be Gaussian through tomographic com-

plete measurements and that Eve is restricted to collective attacks. While the observation of a Gaussian channel is certainly a restriction, it should be noted that this scenario is typically encountered in practise. Moreover, recent work [24, 25] indicates that the Gaussian attack might be optimal for the non-postselected protocols considered here. However, it is still an open problem to relate this result to protocols including announcements and postselection. Furthermore, there is hope to find a quantum de Finetti like argument [26] valid in the regime of continuous variables to extend the security against collective attacks to unconditional security, as this can already be done in finite dimensions. Since we are only interested in the key rate in the asymptotic limit, we do not consider any finite size effects in our analysis. A complete security proof would have to resolve these issues.

We consider a protocol where Alice uses coherent states as signals and send through Eve's domain to Bob, who performs a heterodyne measurement onto the received states. It is known that one can improve the secret key rate if one introduces reverse reconciliation (RR) [1, 8]. This means that Bob decides on a raw key based upon his measurement results and consequently sends Alice correction information over the public channel in the error correction step of the protocol. Another way to improve the performance of the protocol is to employ postselection (PS)[14]: Bob only retains measurement outcomes that are closely correlated to Alice in order to gain some advantage over Eve. This approach can lead to positive secret key rates for direct reconciliation (DR) schemes beyond the so called 3dB loss limit [27]. Since both approaches are not mutual exclusive, we consider combinations of DR and RR with PS. If one takes a realistic error correction protocol into account, it has been shown that it is necessary to introduce a postselection step in the RR protocols to retrieve the initial advantage that RR has over DR [28].

This article is organized as follows. In Sec. II we introduce the QKD protocol under investigation. Then we describe the state distribution scheme in an entanglement based scheme. The fact that state distribution in our protocol can be seen as Alice and Bob performing tomographic complete measurements lets us restrict Eve's knowledge about the signals. This is applied to the Gaussian noisy channel in the next section. In Sec. V we modify our protocol and let Alice and Bob partially announce their measurement outcomes. This defines independent effective binary channels. Next, we calculate a lower bound on the secret key rate for each binary channel independently. The last section contains the numerical optimized secret key rates and our conclusion.

II. THE PROTOCOL

We consider a prepare-and-measure scheme where Alice encodes her bit value into the modulation of coherent states $|\alpha\rangle$ as signals. The complex amplitude $\alpha = \alpha_x + i\alpha_y$ is chosen at random according to a symmetric Gaussian probability distribution

$$p(\alpha) = \frac{1}{2\pi\kappa} \mathrm{e}^{-\frac{|\alpha|^2}{2\kappa}} , \tag{2}$$

centered around the origin. Alice's assigns her signal the bit value 0 (1) if the real part of the sent amplitude α_x is positive (negative). The states $|\alpha\rangle$ are then sent through Eve's domain to Bob. Bob performs a heterodyne measurement on the received states ρ_B^α, which is mathematically equivalent to a projection onto a coherent state $|\beta\rangle = |\beta_x + i\beta_y\rangle$. He obtains the measurement outcome β with probability

$$p(\beta|\alpha) = \frac{1}{\pi}\langle\beta|\rho_B^\alpha|\beta\rangle \tag{3}$$

and assigns a bit value 0 (1) whenever his measurement outcome β_x is positive (negative).

After Bob has measured out the received states, Alice announces partially the amplitude of the sent signals as $a = \{|\alpha_x|, \alpha_y\}$ and Bob announces respectively partially his measurement outcome as $b = \{|\beta_x|, \beta_y\}$. As we will see in Sec. V, this announcement will enable us to decompose the problem into effective independent binary channels.

III. REPLACEMENT OF THE SOURCE AND COMPLETE TOMOGRAPHIC MEASUREMENTS

The starting point of our analysis is that we rephrase the state preparation step in the prepare-and-measure setup in an entanglement based way. This can be done by supplying Alice with a suitable source of entangled states. One part of the entangled state is kept by Alice whereas the other part is sent through the quantum channel to Bob. This scheme is a valid description of the prepare-and-measure scheme, if a measurement performed by Alice onto her part of the entangled state effectively prepares the desired conditional state of the prepare-and-measure scheme with the proper *a priori* probabilities. As we show later, this can be done for the protocol introduced in the previous section. Moreover, both measurements performed by Alice and Bob turn out to be tomographical complete in our case.

After preparing n entangled states, Alice and Bob share the state $\rho_{AB}^{\otimes n}$, since we restrict Eve to collective attacks. Without loss of generality one can assume that ρ_{AB} originates from a pure three party state $|\Psi_{ABE}\rangle$. Eve holds the purifying environment ρ_E of ρ_{AB} which summarizes her knowledge about the distributed states.

As we restrict ourselves to the case when both measurements performed by Alice and Bob are tomographic complete, they can in principle reconstruct their shared state ρ_{AB}. However, we skip details of the tomography in our analysis as we are only interested in evaluating the secret key rate in the asymptotic limit as $n \to \infty$. Therefore, the security analysis presented here can be

considered as incomplete. The aim is to investigate what the rate one can expect to find assuming that one solves the additional steps involving the estimate of the state shared by Alice and Bob.

From the purity of state $|\Psi_{ABE}\rangle$ it follows from Schmidt's decomposition that $\rho_{AB} = \mathrm{tr}_E|\Psi_{ABE}\rangle\langle\Psi_{ABE}|$ and $\rho_E = \mathrm{tr}_{AB}|\Psi_{ABE}\rangle\langle\Psi_{ABE}|$ have the same eigenvalues. Eve's reduced density matrix ρ_E is then determined up to an arbitrary unitary operation on her system by the state tomography. This in turn completely determines Eve's knowledge about the distributed signals.

In the following we apply this kind of analysis to our protocol from Sec. II in a realistic scenario.

IV. APPLICATION TO THE GAUSSIAN CHANNEL

It has been shown by Grosshans *et al.* [8] that Alice's state preparation can formally be described in an entanglement based scheme. It corresponds to a situation where Alice has a source under her control that produces two-mode squeezed states $|\xi_{AB'}\rangle$. If Alice performs a heterodyne measurement onto her part of the state, she effectively prepares a coherent state in the B' system with Gaussian *a priori* probability. As the source of two-mode squeezed states is under her control, she can choose a suitable squeezing parameter so that she indeed effectively prepares coherent states with the proper *a priori* probability (2). The part B' of the state is then passed to Bob through Eve's domain. Bob performs a heterodyne measurement on the received state. Since this measurement is tomographical complete, we can directly apply the reasoning of the last section to this specific protocol and obtain the state in Eve's hand.

For the state tomography step, it is worth noting that Alice's reduced density matrix $\rho_A = \mathrm{tr}\rho_{AB}$ is fixed by preparing coherent states $|\alpha\rangle$ with the *a priori* probabilities given by Eq. (2). One can therefore parameterize Alice's subsystem by the variance κ of the probability distribution $p(\alpha)$. Moreover, it suffices to check the conditional states ρ_B^α to estimate Eve's interference with the signals. However, we do not consider arbitrary noise imposed by Eve on the conditional states, but limit our security analysis to a scenario which is typically encountered in experiments: we assume that the states Bob receives are attenuated by the loss η in the quantum channel and the conditional probability distributions $p(\beta|\alpha)$ as given by Eq. (3) still have Gaussian form but are broadened by a factor

$$\delta = 2\left(\frac{\Delta^2_{\mathrm{obs}}\beta_x}{\Delta^2_{\mathrm{vac}}\beta_x} - 1\right) , \tag{4}$$

the so called excess noise. Here, $\Delta^2_{\mathrm{obs}}\beta_x$ denotes the observed variance of the classical probability distribution (3) and $\Delta^2_{\mathrm{vac}}\beta_x$ is the corresponding variance of the vacuum. We have included the factor 2 so that our definition of the excess noise matches the one given in Ref. [7] via quadrature-‘ measurements. The quadrature operator $\hat{x}$ is defined as $\hat{x} = \frac{1}{\sqrt{2}}(\hat{a} + \hat{a}^\dagger)$, where $\hat{a}$ and $\hat{a}^\dagger$ is the photon annihilation and creation operator. As a further assumption, we suppose that the channel adds the same amount of noise in both quadratures, so that Bob effectively verifies that he receives displaced thermal states as conditional states, denoted by ρ_B^α. Then the probability of Bob getting the measurement outcome β conditioned on Alice sending a coherent state with amplitude α is given by Eq. (3) as

$$p(\beta|\alpha) = \frac{2}{\pi(2+\delta)} \mathrm{e}^{-\frac{2|\beta-\sqrt{\eta}\alpha|^2}{2+\delta}} . \tag{5}$$

Since Bob's subsystem can be characterized by the estimated channel parameters, the total bipartite state ρ_{AB} is given by the input variance κ, the excess noise δ and the loss η. As mentioned before, the knowledge ρ_{AB} determines Eve's quantum state ρ_E up to an arbitrary unitary operation on her system when complete tomographic measurements are available. It then follows that Eve's knowledge about the signals is fixed by the set of parameters κ, η and δ. Therefore, all attacks performed by Eve give her exactly the same amount of information about the signals as long as the channel can be verified to be Gaussian. In particular, this means that attacks like the entangling cloner [8] or the amplifier attack [9, 15] are equivalent in this setting and Eve retains the whole purifying environment. Recent results concerning the optimality of Gaussian attacks, when the full tomographic information is not available, can be found in [24, 25].

Here one can pick a specific attack to construct Eve's ancilla system ρ_E, which is only restricted in the sense that the conditional states ρ_B^α that Bob receives are thermal states and Eve retains the whole purifying environment of ρ_B^α. On the other hand, the joint probability distribution $p(\alpha, \beta)$ of Alice preparing an input state with amplitude α and Bob obtaining a measurement outcome β is fixed by the state tomography. It follows that Eve's conditional states $|\epsilon^{\alpha,\beta}\rangle$ already contain all her knowledge about the distributed signals. These states are pure, since they can be thought of originating from a projection measurement of the pure three party state $|\Psi_{ABE}\rangle$. Equivalently, Eve's information can also summarized in the matrix of all possible overlaps $\langle\epsilon^{\alpha,\beta}|\epsilon^{\alpha',\beta'}\rangle$.

We will proceed to calculate a lower bound on the secret key rate with the specified discretisation to bit-values of continuous outcomes β and α. It turns out that in this case Eve will effectively have to distinguish non-Gaussian states on an infinite dimensional Hilbert space to infer the bit-value. Since this is hard to solve in general, we apply an approach to define effective binary channels as we have already done in [28] and let Alice and Bob partially announce α and β. This partial knowledge will become available to Eve, who then only needs to distinguish two nonorthogonal states on a two dimensional Hilbert space, so that we can evaluate easily all related quantities.

V. EFFECTIVE BINARY CHANNELS

The security analysis presented here is limited to the collective attack scenario, so that the bipartite state between Alice and Bob after n uses of the quantum channel is simply $\rho_{AB}^{\otimes n}$. Consequently, Bob's measurement outcomes β on subsequent signals are independent. Suppose now that Alice announces the modulus of the real part $|\alpha_x|$ and the imaginary part α_y of the prepared amplitude $\alpha = \alpha_x + i\alpha_y$. Now Bob knows that the state he receives can only originate from the two possible states $|\pm|\alpha_x| + i\alpha_y\rangle$ and that in each distributed state one bit of classical information is encoded. Each distribution of a signal between Alice and Bob corresponds to the use of an effective binary channel defined by Alice's announcement and Bob's measurement. From Eq. (2) follows that both possible input states occur with equal probability. The probability of Alice making a certain announcement $a = \{|\alpha_x|, \alpha_y\}$ can be directly calculated form Eq. (2) as

$$\begin{aligned} p(a) &= p(+|\alpha_x| + i\alpha_y) + p(-|\alpha_x| + i\alpha_y) \\ &= 2p(|\alpha_x| + i\alpha_y) = \frac{1}{\pi\kappa} \mathrm{e}^{-\frac{|a|^2}{2\kappa}} \ . \end{aligned} \tag{6}$$

Bob performs a heterodyne measurement on the received state. The probability that he gets the measurement outcome β after the announcement of Alice can be calculated from Eq. (5) as

$$\begin{aligned} p(\beta|a) &= \frac{p(\beta|a,0)p(a,0) + p(\beta|a,1)p(a,1)}{p(a,0) + p(a,1)} \\ &= \frac{1}{2}\left(p(\beta|a,0) + p(\beta|a,1)\right) \ , \end{aligned} \tag{7}$$

where we have characterized the two possible values for the amplitude $\alpha = \pm|\alpha_x| + i\alpha_y$ by the encoded bit-value 0 or 1 and the announcement a. The conditional probabilities for Bob obtaining the measurement result β for given announcement a are directly given by (5) as

$$\begin{aligned} p(\beta|a,0) &= \frac{2}{\pi\,(2+\delta)} \mathrm{e}^{-2\left(\frac{(\beta_x - \sqrt{\eta}|\alpha_x|)^2 + (\beta_y - \sqrt{\eta}\alpha_y)^2}{2+\delta}\right)} \\ p(\beta|a,1) &= \frac{2}{\pi\,(2+\delta)} \mathrm{e}^{-2\left(\frac{(\beta_x + \sqrt{\eta}|\alpha_x|)^2 + (\beta_y - \sqrt{\eta}\alpha_y)^2}{2+\delta}\right)} \ . \end{aligned} \tag{8}$$

Similar to the announcement of Alice, we let Bob record the measured β for each signal and publicly announce $b = \{|\beta_x|, \beta_y\}$. From Eq. (7) follows that

$$p(+|\beta_x| + i\beta_y|a) = p(-|\beta_x| + i\beta_y|a) \ ,$$

so that the probability for Bob making an announcement b given Alice announced a is

$$p(b|a) = 2p(+|\beta_x| + i\beta_y|a). \tag{9}$$

Both announcements of Alice and Bob for a given distributed state will then define one effective binary channel. Furthermore, the error probability for Bob assigning the wrong bit-value can be computed from (8) as

$$\mathrm{e}^{+} = \frac{p(b,+|a,1)}{p(b,+|a,0) + p(b,+|a,1)} \ , \tag{10}$$

where we have chosen to describe Bob's measurement outcome β by the announcement b and the sign of the measured β_x, which corresponds to Bob's decision on a bit-value. Respectively the error probability e^- when he obtained a negative sign for the measured β_x is given by

$$\mathrm{e}^{-} = \frac{p(b,-|a,0)}{p(b,-|a,0) + p(b,-|a,1)} \ . \tag{11}$$

From Eq. (5) follows that each effective binary channel defined by the announcements of a and b is symmetric in the error rate, since

$$e^+ = e^- \equiv e \equiv e(|\alpha_x|, |\beta_x|) = \frac{1}{1 + \mathrm{e}^{\frac{8\sqrt{\eta}|\alpha_x||\beta_x|}{2+\delta}}} \tag{12}$$

holds. Each distributed state between Alice and Bob with announced a and b therefore corresponds to the use of an effective symmetric binary channel with error rate e as given by (12). Each information channel contributes an amount of $1 - H^{\mathrm{bin}}$ to the mutual information between Alice and Bob, whereas H^{bin} is the entropy of a binary symmetric channel,

$$H^{\mathrm{bin}}(e) = -e\,\log_2(e) - (1-e)\,\log_2(1-e). \tag{13}$$

The total mutual information between Alice and Bob $I_{A:B}$ can be calculated as a sum over all effective binary channels weighted with the appropriate probabilities (6) and (9) as

$$\begin{aligned} I_{A:B} = &\int_0^\infty \mathrm{d}|\alpha_x| \int_{-\infty}^\infty \mathrm{d}\alpha_y \ p(a) \times \\ &\times \int_0^\infty \mathrm{d}|\beta_x| \int_{-\infty}^\infty \mathrm{d}\beta_y \ p(b|a) \left[1 - \mathrm{H}^{\mathrm{bin}}\left(e\right)\right] . \end{aligned} \tag{14}$$

Since the error rate e only depends on the announced values of $|\beta_x|$ and $|\alpha_x|$ one can carry out parts of the integration analytically to simplify (14) as

$$\begin{aligned} I_{A:B} = &\int_0^\infty \mathrm{d}|\alpha_x| \ p(|\alpha_x|) \times \\ &\times \int_0^\infty \mathrm{d}|\beta_x| \ p\left(|\beta_x|\big||\alpha_x|\right) \left[1 - \mathrm{H}^{\mathrm{bin}}\left(e\right)\right] . \end{aligned} \tag{15}$$

The total probability $p(|\beta_x|||\alpha_x|)$ that Bob announces a particular value $|\beta_x|$ for a given announcement a of Alice can be derived from (7) and (8) as

$$\begin{aligned} p\left(|\beta_x|\big||\alpha_x|\right) &= \int_{-\infty}^\infty \mathrm{d}\beta_y \ p(b|a) \\ &= \sqrt{\frac{2}{\pi\,(2+\delta)}} \left(e^{-\frac{2(|\beta_x| + \sqrt{\eta}|\alpha_x|)^2}{2+\delta}} + e^{-\frac{2(|\beta_x| - \sqrt{\eta}|\alpha_x|)^2}{2+\delta}}\right) \end{aligned} \tag{16}$$

and the probability that Alice announces $|\alpha_x|$ follows from (6) as

$$p(|\alpha_x|) = \int_{-\infty}^{\infty} \mathrm{d}\alpha_y p(a) = \sqrt{\frac{2}{\pi\kappa}} \mathrm{e}^{-\frac{|\alpha_x|^2}{2\kappa}} \ . \qquad (17)$$

We have now quantified the mutual information between Alice and Bob. As mentioned before, Eve's information about the signals is summarized in holding conditional quantum states $|\epsilon^{\alpha,\beta}\rangle$. The announced values of a and b give her partial information about the distributed signals. In particular, she knows the effective binary channel that has been used by Alice and Bob and the error rate e of that channel. In other words, Eve knows for a given announcement of a and b that she holds a convex combination of the four possible states $|\epsilon^{a,b}_{0,+}\rangle, |\epsilon^{a,b}_{0,-}\rangle, |\epsilon^{a,b}_{1,+}\rangle, |\epsilon^{a,b}_{1,-}\rangle$ in her ancilla system, where 0 (1) corresponds to an encoded bit-value 0 (1) by Alice and + (−) to Bob obtaining a positive (negative) measurement outcome for β_x. The state $\epsilon^{a,b}$ that Eve holds for a given announcement $\{a, b\}$ can thus be written as

$$\begin{aligned}\epsilon^{a,b} =& \frac{1}{2}\Big[(1-e)\left(|\epsilon^{a,b}_{0,+}\rangle\langle\epsilon^{a,b}_{0,+}| + |\epsilon^{a,b}_{1,-}\rangle\langle\epsilon^{a,b}_{1,-}|\right) \\ &+e\left(|\epsilon^{a,b}_{0,-}\rangle\langle\epsilon^{a,b}_{0,-}| + |\epsilon^{a,b}_{1,+}\rangle\langle\epsilon^{a,b}_{1,+}|\right)\Big] \ . \qquad (18)\end{aligned}$$

The state $\epsilon^{a,b}$ can be interpreted as a uniform mixture of states corresponding to different encoded bit-values

$$\epsilon^{a,b} = \frac{1}{2}\left(\epsilon^{a,b}_0 + \epsilon^{a,b}_1\right) \ , \qquad (19)$$

or as a uniform mixture of states corresponding to different signs of the measured β_x

$$\epsilon^{a,b} = \frac{1}{2}\left(\epsilon^{a,b}_+ + \epsilon^{a,b}_-\right) \ , \qquad (20)$$

with

$$\begin{aligned}\epsilon^{a,b}_0 &= (1-e)|\epsilon^{a,b}_{0,+}\rangle\langle\epsilon^{a,b}_{0,+}| + e|\epsilon^{a,b}_{0,-}\rangle\langle\epsilon^{a,b}_{0,-}| \\ \epsilon^{a,b}_1 &= (1-e)|\epsilon^{a,b}_{1,-}\rangle\langle\epsilon^{a,b}_{1,-}| + e|\epsilon^{a,b}_{1,+}\rangle\langle\epsilon^{a,b}_{1,+}| \\ \epsilon^{a,b}_+ &= (1-e)|\epsilon^{a,b}_{0,+}\rangle\langle\epsilon^{a,b}_{0,+}| + e|\epsilon^{a,b}_{1,+}\rangle\langle\epsilon^{a,b}_{1,+}| \\ \epsilon^{a,b}_- &= (1-e)|\epsilon^{a,b}_{1,-}\rangle\langle\epsilon^{a,b}_{1,-}| + e|\epsilon^{a,b}_{0,-}\rangle\langle\epsilon^{a,b}_{0,-}| \ . \qquad (21)\end{aligned}$$

If Eve wants to infer the encoded bit-value, she effectively has to distinguish the states $\epsilon^{a,b}_0$ and $\epsilon^{a,b}_1$. This case is common in QKD and we refer to it as direct reconciliation (DR). As already mentioned, there exists an inequivalent way to distill a key from exchanged quantum states in CV-QKD: with the use of strict one-way communication in the classical post-processing step of the protocol, one can force Eve to infer Bob's measurement outcome rather than the encoded bit-value. This method is called reverse reconciliation and was first pointed out by Grosshans [1, 8]. For the specific protocol investigated here this means that Eve has to discriminate $\epsilon^{a,b}_+$ and $\epsilon^{a,b}_-$ for a given effective binary channel in the RR schemes.

VI. LOWER BOUND ON SECRET KEY RATE

The aim of this article is to compute a achievable lower bound on the secret key rate for our specified prepare-and-measure QKD using coherent states. By now we have shown that Eve's knowledge about the distributed signals, given a certain effective binary channel is used, is summarized in the quantum states $\epsilon^{a,b}_0$ and $\epsilon^{a,b}_1$ for the DR schemes or $\epsilon^{a,b}_+$ and $\epsilon^{a,b}_-$ when RR is applied. In the following, we use a result by Devetak and Winter [21], which gives a lower bound on the secret key rate as a function of the states that Eve has to distinguish. This approach is valid in the collective attack scenario and one-way classical post-processing. Then the secret key rate G is bounded from below by

$$G \geq \mathrm{I}_{A:B} - \chi \ , \qquad (22)$$

with χ being Holevo's quantity [29]. Since we investigate a practical QKD scheme with a specified measurement setup, we have replaced the Holevo quantity between Alice and Bob in theorem (1) of [21] by the classical mutual Information $\mathrm{I}_{A:B}$. The Holevo quantity χ is defined as

$$\begin{aligned}\chi &= S(\overline{\rho}) - \sum_{i=0}^{1} \mathrm{p}_i S(\rho_i) \qquad (23)\\ \overline{\rho} &= \sum_{i=0}^{1} \mathrm{p}_i \rho_i,\end{aligned}$$

where $S(\rho) = -\mathrm{tr}\,(\rho \mathrm{log}_2 \rho)$ denotes the von Neumann entropy and the ρ_i are the states that Eve needs to distinguish. The announcements of a and b divide the state distribution into independent binary channels. It follows that we can apply the bound (23) to each effective binary channel defined by the announcement of a and b separately. The contribution to the mutual information between Alice and Bob per use of an effective binary channel is $1 - H^{\mathrm{bin}}(e)$, where the binary entropy $H^{\mathrm{bin}}(e)$ is given by Eq. (13). An upper bound for Eve's information about the signals for a given announcement can be written according to Eq. (23) as

$$\chi^{a,b}_{DR} = S(\epsilon^{a,b}) - \frac{1}{2}\left[S\left(\epsilon^{a,b}_0\right) + S\left(\epsilon^{a,b}_1\right)\right] \ , \qquad (24)$$

when the key bit is determined by Alice's encoding procedure as in the DR schemes or as

$$\chi^{a,b}_{RR} = S(\epsilon^{a,b}) - \frac{1}{2}\left[S\left(\epsilon^{a,b}_+\right) + S\left(\epsilon^{a,b}_-\right)\right] \ , \qquad (25)$$

when a RR scheme is applied. We have used that the *a priori* probabilities $p_i = \frac{1}{2}$ in a given effective binary channel for both RR and DR, as can be seen from Eqs. (19) and (20). Hence we have to calculate the von Neumann entropies of the states defined in Eqs. (18) and (21) to bound Eve's knowledge about the key. A lower bound can then be obtained with the help of Eqs. (6),

(9) and (13) by summing over all independent effective binary channels as

$$G \geq \int_0^\infty \mathrm{d}|\alpha_x| \int_{-\infty}^\infty \mathrm{d}\alpha_y \; p(a) \int_0^\infty \mathrm{d}|\beta_x| \times \qquad (26)$$
$$\times \int_{-\infty}^\infty \mathrm{d}\beta_y \; p(b|a) \left\{ \left[1 - \mathrm{H}^{\mathrm{bin}}\left(e\right) \right] - \chi^{a,b} \right\} \; ,$$

where the Holevo quantity $\chi^{a,b}$ is given by Eq. (24) in the DR schemes and by Eq. (25) in the RR case. In the following we will explicitly calculate the Holevo quantities for these two types of protocols for a lossy and noisy Gaussian quantum channel.

VII. EVE'S INFORMATION

We have pointed out that all collective attacks that Eve might perform on the distributed signals are unitarily equivalent if the quantum channel between Alice and Bob can be verified as being symmetric and Gaussian, assuming that Eve retains the whole purifying environment. It is convenient to pick a specific attack with these properties to estimate Eve's knowledge about the distributed signals. Here, we have chosen the entangling cloner attack [8] to carry out the calculation. In this attack, Eve taps off the signals sent by Alice with a beam-splitter and feeds one half of a two mode squeezed state in unused port of the beam-splitter. In doing so, the signals become attenuated according to the transmittivity of the beam-splitter and she introduces Gaussian excess noise on Bob's side. The amount of squeezing she uses in preparing her two mode squeezed state relates to the excess noise seen by Bob. More specifically, the state shared between Eve and Bob conditioned on Alice sending a coherent state $|\alpha\rangle$ can be constructed via

$$|\Psi^\alpha_{B,E}\rangle = \hat{R}_{B,E_1}(\eta)\hat{S}_{E_1,E_2}(\xi)|\alpha\rangle_B|0\rangle_{E_1}|0\rangle_{E_2} \; , \qquad (27)$$

with

$$\hat{R}_{B,E_1}(\theta) = e^{\frac{\theta}{2}(\hat{e_1}^\dagger \hat{b} - \hat{b}^\dagger \hat{e_1})} \qquad (28)$$
$$\hat{S}_{E_1,E_2}(\xi) = e^{-\xi \hat{e_1}^\dagger \hat{e_2}^\dagger + \xi^* \hat{e_2}\hat{e_1}} \; ,$$

whereas E_1, E_2 label the modes in Eve's hand, $\hat{S}_{E_1,E_2}(\xi)$ denotes the two-mode squeezing operator with squeezing parameter $\xi = r\mathrm{e}^{i\phi}$ as can be found, for example, in Ref. [30]. The unitary $\hat{R}_{B,E_1}(\theta)$ is associated to a beam-splitter with transmittivity η via the identification $\sqrt{\eta} = \cos(\frac{\theta}{2})$. The operators $\hat{b}, \hat{e_1}$ and $\hat{e_2}$ are the bosonic anihilation operators associated with the modes E_1, E_2 and B. From this, one can calculate Bob's received states by tracing out Eve's subsystem. It is easy to see that from Bob's point of view Eve effectively injects a thermal state in the beam-splitter so that Bob will observe Gaussian noise. The amount of excess noise δ is related to the squeezing parameter $\xi = r\mathrm{e}^{i\gamma}$ as $\delta = 2\sinh^2\mathrm{r}(1-\eta)$.

From Eq. (27), one can calculate Eve's states $|\epsilon^{\alpha,\beta}\rangle$ conditioned on Alice sending a coherent state $|\alpha\rangle$ and Bob obtaining the measurement outcome β by projecting $|\Psi^\alpha_{B,E}\rangle$ onto $|\beta\rangle$. As before, we relabel the state $|\epsilon^{\alpha,\beta}\rangle$ in terms of the announcement $\{a,b\}$, the encoded bit-value $i \in \{0,1\}$ and the sign of Bob's measurement outcome $k \in \{+,-\}$ as $|\epsilon^{a,b}_{i,k}\rangle$. Since Eve's system is fixed up to an arbitrary global unitary on her system by the tomography step, it is sufficient to calculate the matrix of all possible overlaps $\langle\epsilon^{a,b}_{i,k}|\epsilon^{a,b}_{j,l}\rangle$ to estimate Eve's knowledge. It turns out that the overlaps can be written as

$$\langle\epsilon^{a,b}_{i,k}|\epsilon^{a,b}_{j,l}\rangle = \qquad (29)$$
$$= \begin{pmatrix} 1 & Be^{-i\phi} & Ae^{i\psi} & ABe^{i\psi-i\phi} \\ Be^{i\phi} & 1 & ABe^{i\psi+i\phi} & Ae^{i\psi} \\ Ae^{-i\psi} & ABe^{-i\psi-i\phi} & 1 & BBe^{-i\phi} \\ ABe^{-i\psi+i\phi} & Ae^{-i\psi} & Be^{i\phi} & 1 \end{pmatrix} \qquad (30)$$

with

$$A = \mathrm{e}^{-\left(\alpha_x^2\left(1-\frac{\eta}{1+\delta}\right)\right)} \qquad (31)$$
$$B = \mathrm{e}^{-\left(\beta_x^2\frac{\delta}{1+\delta}\right)} \; .$$

One can get rid of the phase factors depending on ϕ and ψ by multiplying the states $|\epsilon^{a,b}_{i,k}\rangle$ by appropriate phase factors. This is possible, since we are only interested in the construction of states of the form

$$\rho = \sum_{i,k} p(i,k)|\epsilon^{a,b}_{i,k}\rangle\langle\epsilon^{a,b}_{i,k}| \; , \qquad (32)$$

as can be seen from Eqs. (18) and (21). The states ρ are obviously invariant under this transformation.

The matrix of overlaps (29) is then of the form

$$\langle\epsilon^{a,b}_{i,k}|\epsilon^{a,b}_{j,l}\rangle = \begin{pmatrix} 1 & B & A & AB \\ B & 1 & AB & A \\ A & AB & 1 & B \\ AB & A & B & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & A \\ A & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & B \\ B & 1 \end{pmatrix} \; . \qquad (33)$$

From that it follows that one can write the states $|\epsilon^{a,b}_{i,k}\rangle$ as

$$|\epsilon^{a,b}_{i,k}\rangle = |\epsilon^{a,b}_i\rangle|\epsilon^{a,b}_k\rangle \qquad (34)$$

with

$$\langle\epsilon^{a,b}_0|\epsilon^{a,b}_1\rangle = A = \mathrm{e}^{-\left(\alpha_x^2\left(1-\frac{\eta}{1+\delta}\right)\right)} \qquad (35)$$
$$\langle\epsilon^{a,b}_+|\epsilon^{a,b}_-\rangle = B = \mathrm{e}^{-\left(\beta_x^2\frac{\delta}{1+\delta}\right)},$$

where we already replaced the squeezing parameter ξ by the excess noise δ observed by Bob.

Since the states under investigation can be written as a product (34) of two states in two dimensional Hilbert

spaces, one can expand them as

$$|\epsilon_0^{a,b}\rangle = c_0|\Phi_0\rangle + c_1|\Phi_1\rangle \quad (36)$$
$$|\epsilon_1^{a,b}\rangle = c_0|\Phi_0\rangle - c_1|\Phi_1\rangle \quad (37)$$

and

$$|\epsilon_+^{a,b}\rangle = c_+|\Phi_+\rangle + c_-|\Phi_-\rangle \quad (38)$$
$$|\epsilon_-^{a,b}\rangle = c_+|\Phi_+\rangle - c_-|\Phi_-\rangle\ , \quad (39)$$

where $|\Phi_0\rangle$ and $|\Phi_1\rangle$ form a set of orthonormal basis states for the Hilbert space spanned by $|\epsilon_0^{a,b}\rangle$ and $|\epsilon_1^{a,b}\rangle$. Respectively $|\Phi_+\rangle$ and $|\Phi_-\rangle$ form an orthogonal basis for the space spanned by $|\epsilon_+^{a,b}\rangle$ and $|\epsilon_-^{a,b}\rangle$. The coefficients c_0, c_1, c_+ and c_- depend on the effective binary channel labeled by a and b, though we suppress these indices now to simplify the notation. It is important, however, to keep in mind that we estimate Eve's knowledge about the signals for each effective channel independently. The normalization condition reads

$$|c_0|^2 + |c_1|^2 = |c_+|^2 + |c_-|^2 = 1. \quad (40)$$

and

$$|c_0|^2 - |c_1|^2 = \langle\epsilon_0^{a,b}|\epsilon_1^{a,b}\rangle = A \quad (41)$$
$$|c_+|^2 - |c_-|^2 = \langle\epsilon_+^{a,b}|\epsilon_-^{a,b}\rangle = B$$

is fixed by the overlaps (35). In this basis the state $\epsilon^{a,b}$ of Eq. (18) can be written as

$$\epsilon^{a,b} = \begin{pmatrix} |c_0|^2|c_+|^2 & 0 & 0 & (1-2e)c_0c_1^*c_+c_-^* \\ 0 & |c_0|^2|c_-|^2 & (1-2e)c_0c_1^*c_+c_-^* & 0 \\ 0 & (1-2e)c_0^*c_1c_+^*c_- & |c_1|^2|c_+|^2 & 0 \\ (1-2e)c_0^*c_1c_+^*c_- & 0 & 0 & |c_1|^2|c_-|^2 \end{pmatrix}, \quad (42)$$

which has the eigenvalues

$$\lambda_{1,2} = \frac{1}{2}\left[|c_0|^2|c_-|^2 + |c_1|^2|c_+|^2 \pm \sqrt{\left(|c_0|^2|c_-|^2 + |c_1|^2|c_+|^2\right)^2 - 16e(1-e)|c_0|^2|c_-|^2|c_1|^2|c_+|^2}\right] \quad (43)$$
$$\lambda_{3,4} = \frac{1}{2}\left[|c_0|^2|c_+|^2 + |c_1|^2|c_-|^2 \pm \sqrt{\left(|c_0|^2|c_+|^2 + |c_1|^2|c_-|^2\right)^2 - 16e(1-e)|c_0|^2|c_-|^2|c_1|^2|c_+|^2}\right]\ ,$$

so that we can calculate the first term of Eqs. (24) and (25) with the help of Eqs. (43),(41),(40) and (35) via the equation

$$S(\epsilon^{a,b}) = -\sum_i \lambda_i \log_2 \lambda_i\ . \quad (44)$$

The explicit expression is omitted here.

A. Direct reconciliation

In the DR protocols, Eve has to discriminate the states $\epsilon_0^{a,b}$ and $\epsilon_1^{a,b}$ as defined in Eqs. (21) in order to infer the bit-value encoded by Alice. These can be expressed in product form (34) as

$$\epsilon_0^{a,b} = |\epsilon_0^{a,b}\rangle\langle\epsilon_0^{a,b}| \otimes \left[(1-e)|\epsilon_+^{a,b}\rangle\langle\epsilon_+^{a,b}| + e|\epsilon_-^{a,b}\rangle\langle\epsilon_-^{a,b}|\right] \quad (45)$$
$$\epsilon_1^{a,b} = |\epsilon_1^{a,b}\rangle\langle\epsilon_1^{a,b}| \otimes \left[(1-e)|\epsilon_-^{a,b}\rangle\langle\epsilon_-^{a,b}| + e|\epsilon_+^{a,b}\rangle\langle\epsilon_+^{a,b}|\right]\ .$$

With the help of the basis states $|\Phi_0\rangle$, $|\Phi_1\rangle$ and $|\Phi_+\rangle$, $|\Phi_-\rangle$ these states can be written as

$$\epsilon_0^{a,b} = \begin{pmatrix} |c_0|^2 & c_1^*c_0 \\ c_0^*c_1 & |c_1|^2 \end{pmatrix} \otimes \begin{pmatrix} |c_+|^2 & (1-2e)\,c_+^*c_- \\ (1-2e)\,c_-^*c_+ & |c_-|^2 \end{pmatrix} \quad (46)$$
$$\epsilon_1^{a,b} = \begin{pmatrix} |c_0|^2 & -c_1^*c_0 \\ -c_0^*c_1 & |c_1|^2 \end{pmatrix} \otimes \begin{pmatrix} |c_+|^2 & -(1-2e)\,c_+^*c_- \\ -(1-2e)\,c_-^*c_+ & |c_-|^2 \end{pmatrix}.$$

It is easy to see that there exists a unitary U with $\epsilon_0^{a,b} = U\epsilon_1^{a,b}U^\dagger$, so that $S(\epsilon_0^{a,b}) = S(\epsilon_1^{a,b})$. The eigenvalues of the state $\epsilon_0^{a,b}$ can be obtained by first diagonalizing the

sub-matrices and then taking the tensor product. Then $\epsilon_0^{a,b}$ reads,

$$\epsilon_0^{a,b} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} \lambda_1^0 & 0 \\ 0 & \lambda_2^0 \end{pmatrix} \tag{47}$$

in its eigenbasis. The eigenvalues $\lambda_{1,2}^0$ are given by

$$\lambda_{1,2}^0 = \frac{1}{2}\left(1 \pm \sqrt{1 - 16e(1-e)(|c_+|^2\,|c_-|^2)}\right) . \tag{48}$$

so that the entropy $S(\epsilon_0^{a,b})$ can be computed with the help of Eqs. (12), (35), (41) and (48) and Eve's knowledge about the distributed signals in the DR protocol is upper bounded by

$$\chi_{DR}^{a,b} = S(\epsilon^{a,b}) - S(\epsilon_0^{a,b}) , \tag{49}$$

where again the explicit expression is omitted.

B. Reverse reconciliation

In the RR schemes, the key bits are determined by the sign of Bob's measured β_x component. Hence, Eve has to discriminate the corresponding states $\epsilon_+^{a,b}$ and $\epsilon_-^{a,b}$ (21) for a given effective binary channel. These can be written with the help of Eq. (34) as

$$\begin{aligned} \epsilon_+^{a,b} &= |\epsilon_+^{a,b}\rangle\langle\epsilon_+^{a,b}| \otimes \Big[(1-e)|\epsilon_0^{a,b}\rangle\langle\epsilon_0^{a,b}| + e|\epsilon_1^{a,b}\rangle\langle\epsilon_1^{a,b}|\Big] \\ \epsilon_-^{a,b} &= |\epsilon_-^{a,b}\rangle\langle\epsilon_-^{a,b}| \otimes \Big[(1-e)|\epsilon_1^{a,b}\rangle\langle\epsilon_1^{a,b}| + e|\epsilon_0^{a,b}\rangle\langle\epsilon_0^{a,b}|\Big] . \end{aligned} \tag{50}$$

In the $|\Phi_0\rangle$, $|\Phi_1\rangle$ and $|\Phi_+\rangle$, $|\Phi_-\rangle$basis, these states read

$$\epsilon_+^{a,b} = \begin{pmatrix} |c_+|^2 & c_-^* c_+ \\ c_+^* c_- & |c_+|^2 \end{pmatrix} \otimes \begin{pmatrix} |c_0|^2 & (1-2e)\, c_0^* c_1 \\ (1-2e)\, c_1^* c_0 & |c_1|^2 \end{pmatrix} \tag{51}$$

$$\epsilon_-^{a,b} = \begin{pmatrix} |c_+|^2 & -c_-^* c_+ \\ -c_+^* c_- & |c_-|^2 \end{pmatrix} \otimes \begin{pmatrix} |c_0|^2 & -(1-2e)\, c_0^* c_1 \\ -(1-2e)\, c_1^* c_0 & |c_1|^2 \end{pmatrix} .$$

Similar as in the previous subsection, the states $\epsilon_+^{a,b}$ and $\epsilon_+^{a,b}$ are unitarily equivalent, so that it suffices to calculate $S(\epsilon_+^{a,b})$ to determine the upper bound (25) of Eve's information about the signals for the RR protocols. The eigenvalues $\lambda_{1,2}^+$ of $\epsilon_+^{a,b}$ turn out to be

$$\lambda_{1,2}^+ = \frac{1}{2}\left(1 \pm \sqrt{1 - 16e(1-e)(|c_0|^2\,|c_1|^2)}\right) , \tag{52}$$

so that we can easily estimate Eve's knowledge about the distributed states with the help of Eqs. (52)and (44) as

$$\chi_{RR}^{a,b} = S(\epsilon^{a,b}) - S(\epsilon_+^{a,b}) . \tag{53}$$

VIII. SECRET KEY RATE AND POSTSELECTION

By now, we have calculated the individual terms of an upper bound $\chi^{a,b}$ on Eve's information about the raw key for DR and for RR protocols, given that an effective information channel is used. We have also shown that the mutual information shared between the two honest parties per effective binary channel labeled by the announcement of a and b is given by $1 - H^{\rm bin}$, with $H^{\rm bin}$ being the entropy of a symmetric binary channel (13). The total secret key rate can thus be calculated as a sum over all binary channels according to Eq. (26). Since neither the mutual information $(1 - H^{\rm bin})$ between Alice and Bob nor Eve's information $\chi^{a,b}$ depend on the announced values of α_y and β_y, one can simplify Eq. (26) as

$$\begin{aligned} G &\geq \int_0^\infty {\rm d}|\alpha_x|\; p(|\alpha_x|) \int_0^\infty {\rm d}|\beta_x|\; p(|\beta_x||\alpha_x|) \times \\ &\quad \times \left[1 - {\rm H}^{\rm bin}(e) - \chi^{a,b}\right] \\ &= \int_0^\infty {\rm d}|\alpha_x|\; p(|\alpha_x|) \int_0^\infty {\rm d}|\beta_x|\; p(|\beta_x||\alpha_x|) \Delta I(a,b) , \end{aligned} \tag{54}$$

where the probabilities $p(|\alpha_x|)$ and $p(|\beta_x||\alpha_x|)$ are given by Eqs. (17) and (16).

The term $\Delta I(a,b)$ quantifies the average information theoretic advantage of Alice and Bob over Eve for a given effective channel. Since we have calculated this quantity for all channels separately, we can improve the performance of the protocols by dismissing effective channels whenever $\Delta I(a,b)$ is negative and hence Eve knows more about the distributed signals than Alice and Bob. This procedure is called postselection. Even in absence of noise, a postselection procedure is for example necessary to lead to a positive secret key rate beyond 3 dB losses for

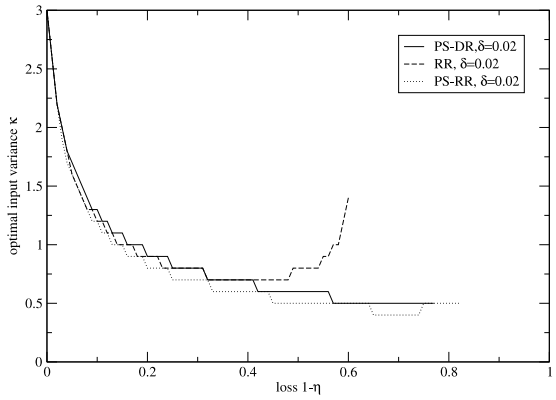

FIG. 1: Optimal values for the input variance κ vs. loss $1-\eta$ for various protocols. All graphs shown correspond to an excess noise δ of 2%.

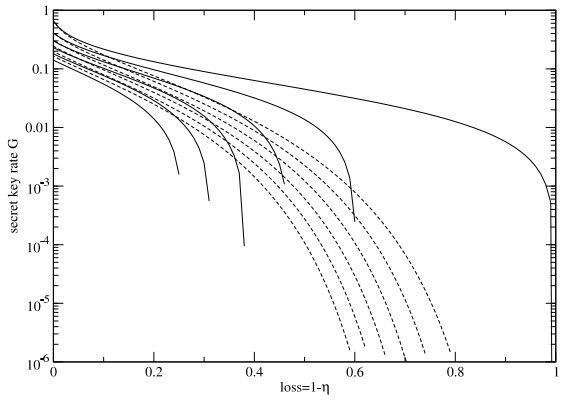

FIG. 2: Comparison of the secret key rate G versus loss $1-\eta$ for the PS-DR (dashed lines) and the RR (solid lines) scheme. The secret key rates shown correspond to an excess noise δ of $\{0, 0.02, 0.04, 0.06, 0.08, 0.1\}$ and decrease with increasing excess noise.

the DR protocols [2]. For RR schemes, all effective binary channels contribute a positive amount to the secret key rate, if one only takes losses in the quantum channel into account [28]. In this scenario, postselecting the measurement outcomes cannot improve the secret key rate. This is however no longer true if the channel imposes excess noise δ on the signals, so that postselection can improve the performance of the RR schemes in this more general setting.

IX. NUMERICAL RESULTS AND DISCUSSION

Now we have everything at hand to evaluate the secret key rate G numerically. For a given excess noise δ and transmission η we can optimize the input variance κ for best performance. Optimal values for the input variance κ are given in Fig. (1). For numerical purposes, we restrict ourselves to vary the variance κ between 0.1 and 3. The optimal variance κ diverges in the limit $\eta \to 1$. Apart from that, the optimal variances fall well inside the region in which we optimize κ.

Fig. (2) shows our results for the RR and the postselected DR scheme. As expected, the secret key rate G decreases with increasing excess noise $\delta = \{0, 0.02, 0.04, 0.06, 0.08, 0.1\}$. However, the noise affects the non-postselected RR scheme much stronger than the postselected DR scheme (PS-DR). The RR protocol looses most of its initial advantage even for a low excess noise of 2 %. This can be counteracted by introducing a postselection step in the RR protocols, as proposed in [28].

After introducing a postselection step in the RR scheme (PS-RR), the protocol performs more robustly against increasing excess noise δ, as can be seen in Fig. (3). Now the PS-RR scheme performs better than the

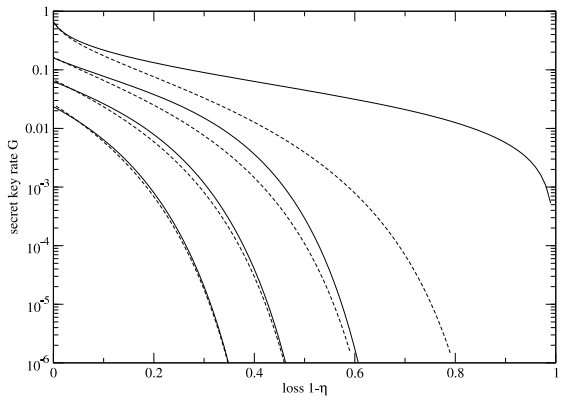

FIG. 3: Combination of postselection and reverse reconciliation. Secret key rates G are plotted for the PS-DR (dashed lines) and the PS-RR (solid lines) protocols and versus the channel loss $1-\eta$. The excess noise δ varies as $\delta = \{0, 0.1, 0.2, 0.3\}$.

DR counterpart for all values of the excess noise, though the behavior of the secret rate gets more and more similar for increasing excess noise. This shows again that it is advantageous to combine postselection with reverse reconciliation for best performance in the presence of Gaussian noisy quantum channels. However, here we assume that all observed excess noise occurs in the quantum channel and can therefore be exploited by Eve. As a benchmark, one can tolerate an excess noise of about $\delta = 0.2$ if the quantum channel has 50% transmittivity. It follows that the applicability of the protocols is very limited with this

conservative assumption.

A. Two-way communication

The security analysis presented here assumes that the communication between Alice and Bob in the classical post-processing step is strictly one-way. From a practical point of view however, it is favorable to give lower bounds to the secret key rate G for two-way communication, since these kind of protocols can easily be implemented with known error correction procedures like CASCADE. In principle, the bound (22) requires one-way communication to be used. This can be circumvented however, if one reveals all information to Eve that is in principle obtainable by an eavesdropper when two-way classical post-processing is used. Following earlier treatment in Ref. [31], one can assume for two-way error correction the worst-case scenario in which the precise position of the errors in Bob's data become publicly known. Then it does not matter anymore, whether Alice or whether Bob make subsequent announcements. Note that in CASCADE, Bob's announcements are completely determined by the error position, and therefore no longer need to be taken into account when calculating the cost of error correction. Given this knowledge, Eve can update the state $\epsilon^{a,b}$ (18) that summarizes her knowledge about the distributed signals and the remaining communication can be chosen to be one-way. Then Eq. (22) is again valid, but the states $\epsilon^{a,b}$ now include this additional information. It follows that Eve either holds the state

$$\epsilon^{a,b}_{\text{no error}} = \frac{1}{2}\left(|\epsilon^{a,b}_{0,+}\rangle\langle\epsilon^{a,b}_{0,+}| + |\epsilon^{a,b}_{1,-}\rangle\langle\epsilon^{a,b}_{1,-}|\right) \tag{55}$$

or

$$\epsilon^{a,b}_{\text{error}} = \frac{1}{2}\left(|\epsilon^{a,b}_{0,-}\rangle\langle\epsilon^{a,b}_{0,-}| + |\epsilon^{a,b}_{1,+}\rangle\langle\epsilon^{a,b}_{1,+}|\right) \tag{56}$$

in her ancilla system. Obviously, the probability that an error in the bit assignment occurs is given by e. It is then easy to show that Eve's information about the signals for a given announcement (a,b) is bounded by

$$\begin{aligned}\chi^{a,b}_{2-\text{way}} &= e\chi^{a,b}_{\text{error}} + (1-e)\chi^{a,b}_{\text{no error}} \\ &= eS\left(\epsilon^{a,b}_{\text{error}}\right) + (1-e)S\left(\epsilon^{a,b}_{\text{no error}}\right)\ ,\end{aligned} \tag{57}$$

whereas the second line follows from the fact that here Eve has to distinguish pure states. Furthermore, since $\epsilon^{a,b}_{\text{no error}}$ and $\epsilon^{a,b}_{\text{error}}$ are unitarily equivalent, $S\left(\epsilon^{a,b}_{\text{error}}\right) = S\left(\epsilon^{a,b}_{\text{no error}}\right)$ and

$$\chi^{a,b}_{2-\text{way}} = S\left(\epsilon^{a,b}_{\text{error}}\right) = S\left(\epsilon^{a,b}_{\text{no error}}\right)\ . \tag{58}$$

The entropy $S\left(\epsilon^{a,b}_{\text{no error}}\right)$ is given by the eigenvalues $\lambda^{2-way}_{1,2}$ of $\epsilon^{a,b}_{\text{no error}}$ (55). It is straight forward to show that these are given by

$$\begin{aligned}\lambda^{2-way}_1 &= |c_0|^2|c_-|^2 + |c_1|^2|c_+|^2 \\ \lambda^{2-way}_2 &= |c_0|^2|c_+|^2 + |c_1|^2|c_-|^2\end{aligned} \tag{59}$$

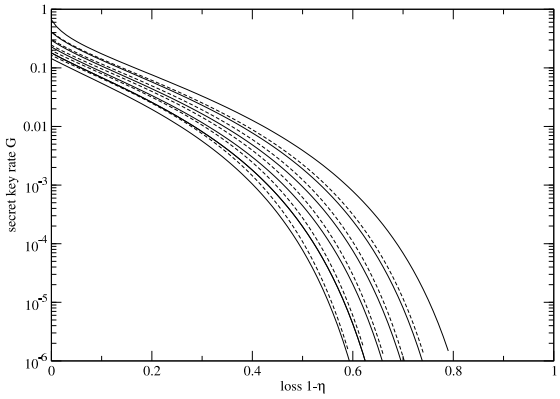

FIG. 4: Secret key rates G for postselected protocols and two-way communication (solid lines) in comparison to the one-way PS-DR protocol (dashed lines). The excess noise δ varies between 0 and 0.1 as in Fig. (2). For $\delta = 0$, the curve for two-way communication coincides with the one for the PS-DR protocol.

with $|c_0|^2, |c_-|^2, |c_1|^2, |c_+|^2$ implicitly given by Eqs.(40) and (41).

Figure (4) shows our numerical results for the secret key rate G with two-way communication in comparison to the postselected DR results. If there is no channel excess noise δ present, we recover our previous result that the DR-PS rate coincides with the two-way rate [28]. Moreover it can be seen that the knowledge about the error positions does not improve Eve's position significantly in our analysis. Even in the presence of excess noise δ, the DR-PS rate gives a good approximation to the two-way bound. A practical implementation using two-way error correction codes like CASCADE will therefore yield a secret key rate close to the one-way DR-PS rate.

B. Practical error correction

We extend our analysis presented here to a more realistic scenario and take the effect of a non-ideal error correction procedure into account.

The key rate (54) gives the theoretical achievable key rate if a perfect error correction procedure is available. In practise however, error correction codes that work exactly at this so called Shannon limit [32] are not known. Realistic error correction codes, like CASCADE [33] work close to that limit. This can be included by modifying Eq. (54) as

$$\begin{aligned}G \geq \int_0^\infty \mathrm{d}|\alpha_x|\ p(|\alpha_x|) \int_0^\infty \mathrm{d}|\beta_x|\ p(|\beta_x||\alpha_x|)\times \\ \times\left[1 - f(e)\mathrm{H}^{\text{bin}}(e) - \chi^{a,b}\right]\ ,\end{aligned} \tag{60}$$

e	$f(e)$
0.01	1.16
0.05	1.16
0.1	1.22
0.15	1.32

TABLE I: Efficiency of Cascade [33] for different values of the error rate e

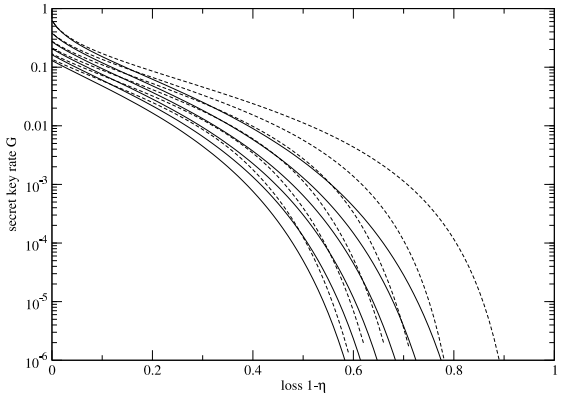

FIG. 5: Secret key rates G for postselected protocols using the two-way error correction scheme CASCADE (solid lines). For comparison, key rates for the PS-RR protocol with one-way codes, that are as efficient as CASCADE are also shown (dashed lines). The excess noise δ varies between 0 and 0.1 as in Fig. (2).

where the function $f(e)$ represents the efficiency of the error correction procedure and is a function of the error rate e. As a benchmark, we assume that the used error correction is as efficient as CASCADE. For our numerical evaluation, we therefore use a linear fit to the values given in Table I. For two-way communication, Eve's knowledge $\chi^{a,b}$ in Eq. (60) is given by Eq. (58). Following this approach, we can give secret key rates which are attainable with todays technology. Numerical results are shown in Fig. (5).

Reverse reconciliation clearly requires one-way communication. On the other hand, developing practical and efficient one-way codes is still work in progress. It is therefore interesting to see how much secret key rate one would gain if one applies a one-way code that is as efficient as CASCADE. This can easily computed via Eq. (60) whereas $\chi^{a,b}$ is given by Eq. (49) for the DR protocol or by Eq. (53) for the RR scheme.

Fig. (5) shows also a comparison between two-way protocols and PS-RR. The error correction procedure is assumed to have the same efficiency as CASCADE. It can be seen that one-way PS-RR has a significant advantage over the attainable two-way protocol only for very low values of the channel excess noise δ. This indicates that the development of efficient one-way codes, as currently under investigation by several groups, will significantly benefit RR protocols if the channel excess noise can be assumed to be of the order of a few percent.

X. CONCLUSION

In conclusion, we have addressed security issues for a CV-QKD scheme in a practical setting. It is important to include a postselection procedure in both the RR and DR schemes to ensure that the protocols perform robust against Gaussian excess noise.

We have shown that a implementation using two-way error correction yields a secret key rate close to the rate of the one-way direct reconciled protocol. As the excess noise increases, the secret key rates for the one-way direct or reverse reconciled protocols become more and maore similar to the ones obtainable by two-way communication. Finally, we compute the secret key rate for a protocol that is readily implementable using the error correction code CASCADE.

XI. ACKNOWLEDGEMENTS

We thank Frederic Grosshans for helpful discussions. This work has been supported by the EU-IST network SECOQC, and the German Research Council (DFG) under the Emmy-Noether program.

[1] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, Nature **421**, 238 (2003).
[2] C. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002).
[3] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (1999).
[4] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[5] T. Hirano, , H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A **68**, 042331 (2003).
[6] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).
[7] R. Namiki and T. Hirano, Phys. Rev. Lett. **92**, 117901 (2004).
[8] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Information and Computation **3**, 535 (2003).
[9] R. Namiki and T. Hirano, Phys. Rev. A **72**, 024301 (2005).
[10] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).
[11] M. Navascués and A. Acín, Phys. Rev. Lett. **94**, 020505

(2005).
[12] R. Namiki and T. Hirano, Phys. Rev. A **67**, 022308 (2003).
[13] S. Iblisdir, G. Van Assche, and N. J. Cerf, Phys. Rev. Lett. **93**, 170502 (2004).
[14] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[15] R. Namiki, M. Koashi, and N. Imoto, Phys. Rev. A **73**, 032302 (2006).
[16] G. Van Assche, S. Iblisbir, and N. J. Cerf, Phys. Rev. A **71**, 052304 (2005).
[17] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[18] M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. A **71**, 022306 (2005).
[19] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[20] C. H. Bennett, G. Brassard, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[21] I. Devetak and A. Winter, Proc. of the Roy. Soc. of London Series A **461**, 207 (2005).
[22] S. K. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. B **79**, 273 (2004).
[23] S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs, Phys. Rev. A **74**, 042326 (2006), quant-ph/0603271.
[24] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[25] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (06).
[26] R. Renner, Ph.D. thesis, ETH Zürich (2005).
[27] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[28] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2006).
[29] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).
[30] S. M. Barnett and P. M. Radmore, *Methods in Theoretical Quantum Optics* (Clarendon Press, 1997).
[31] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).
[32] C. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[33] G. Brassard and L. Salvail, in *Advances in Cryptology - EUROCRYPT '93*, edited by T. Helleseth (Springer, Berlin, 1994), vol. 765 of *Lecture Notes in Computer Science*, pp. 410–423.